David W Mitchell

Dr. Phil Lunsford

ICTN 4040 601

April 14, 2013

Email Security

Individuals, small business, and governments use email to communicate with each other, internally and externally on a daily basis. Some of these confidential emails are directed at a specific person or group. The end user expect for this electronic message to be secure as it transmit to the intended parties. This paper will talk about several steps you can take in email security. One step requires that the end user apply security patches and correct email setting. Encryption with S/MIME is a method to ensure security email transmission. Governments have added additional security features of two-factor authentication. Virtual private network have provide secure transmission of email for remote company employees. The implementation of basic security practices will help your email to be secure during transmission.

The immediate demand to access your email through smart phones, webmail, and corporate virtual private networks for teleworkers have increase the need for email security. Email is a widely used tool to communicate in today's society. Email has become the primary attack vector for attackers according to a Cisco Security White Paper. Attackers have use spam, viruses, phishing, and spyware through email to affect or gain information from an end user.

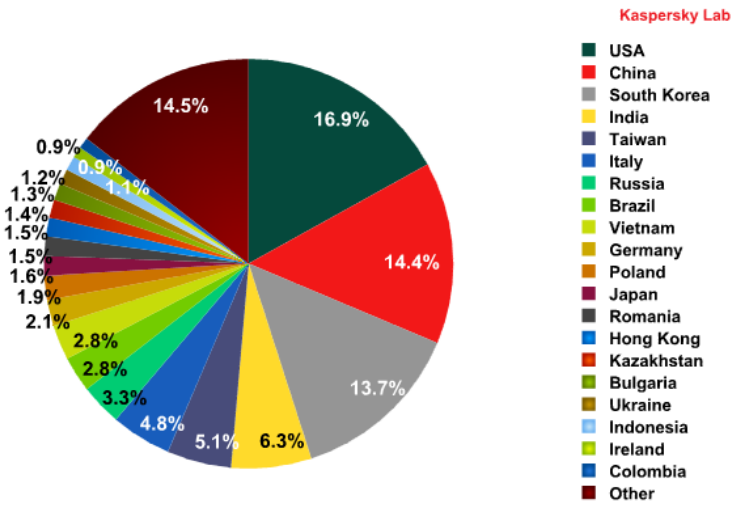

Figure 1: Spam report by country from Kaspersky Lab in February 2013.

Spam is consider any unsolicited email that is normally send through a mass mailing to a large group of email accounts. This email marketing was very inexpensive for companies to market their products. According the Kaspersky Lab Report conduct in February 2013, the United States have lead the sources of spam worldwide with 16.9% as indicated in figure 1. The United States and China have produced more than 31% of the spam worldwide. South Korea had over 50% of the spam produced in January 2013 but decrease to 14% in February. Companies have been able to counter some of the spam with spam filters. Spam filters are used to compare some parameter in email to a list of rules. Spam has moved from just annoying commercial emails to being embedded with malicious code like viruses, Trojans, or phishing from attackers. The malicious code is capable of infiltrate a computer system without their end user's knowledge.

Viruses are sent in email as an attachment and can cause companies to loss productivity and lots of money. For example, the Sobig.F virus spread to 134 counties in four days. (Leyden) It cost many British businesses hundreds of millions in lost revenue. It had affect one out of

every 17 emails sent that day. The virus had modified the Windows registry so the worm would launch when Windows is started. The virus would search for email addresses on the computer and sent out copies of the worm to other email addresses. Worms often look for some type of email to exploit so it can spread the virus. End users can eliminate the worms from spreading by not opening attachments from strangers. Another way to eliminate the spreading of worms is to not open attachment that you didn't request. You can implement mandatory digital signatures in email to assist with eliminating the worms from spreading.

Trojans are malicious code that infect computers so they can obtain information, harm computers, or create backdoor. Backdoors allow hackers easy access to the end user's computer system. The banking Trojan create a fake Adobe Flash Player update for the end user while taking money out of their online bank account according to Tech News Daily. (Weitzenkorn) This was done by redirecting the end user to websites with more malicious code when they installed the fake Adobe update. Trojans allows the hacker to steal information, infect computer, and disable applications according to Michael Erbschloe's journal. (Erbschloe) Erbscholoe talks about combating the Trojans by installing system patches, setting standards for security policies, and using virus scans.

Figure 2: Example of phishing email from Microsoft Safety and Security Center website.

Cybercriminals have used phishing emails and social engineering to obtain information from an end user so they can steal their information or gain money from them. An example of a phishing email is shown in figure 2. End user are directed to fake site that looks exactly the same as an original site in phishing. In March 2012, a phishing gang stole $1.6M life savings of a victim according to NBC News. The gang tricked people to provide their banking information to a fake banking website by send them an email that directed them to a fake site. A computer can be protected from phishing by installing spam filters, anti-virus and firewalls. A person should never enter their banking information in a non-secure site. An end user should avoid clicking links in email that is not familiar. Spear-Phishing makes the email seem as though it had come from someone known by the end user.

Another email security concern is spyware. Spyware is used for advertisements, collecting personal information, tracking and changing computer configuration without the end user's knowledge. Spyware can perform some simple tasks such as changing your homepage settings for a web browser. The end user will not be able to change it back from the homepage site that was set by the spyware. RAT has been used in the past as a remote access Trojan that give a hacker access to your computer system. (Aycock) It has also been used as a tool for help desk or system administrators to assist with troubleshoot problems at remote location. The important value of information is the main reason spyware is in existence according to John Aycock. Software spyware dates back to around 1994. In March 2011, a man in Austin installed spyware on his wife's computer that allow him to view her emails, photos, and mobile telephone records.

There are some basic things you can do to protect against email spyware. The first includes blocking some file types that are known to have viruses such as exe, bat, vbs, and etc.

Secondly, an end user should block any file that have more than one file extension type. Viruses attempt to disguise their executable with double file extension. Some anti-virus products can provide protection against spyware. Two-factor authentication allows the end user to protect his information by requiring more than just something he or she knows but something he or she has. Military uses two-factor authentication with their systems today by requiring a common access card and a password.

Secure Multipurpose Internet Mail Extension also called S/MIME provides email security by encrypting emails that are sent by the end user. (Whitman and Mattord) S/MIME provides cryptographic security to emails. It provides the authentication, non-repudiation and integrity. Digital signatures through S/MIME is provide to add integrity to the email. S/MIME requires protocols such as POP3 and IMAP to operate. An end user is allow to send plain text or encrypted emails using S/MIME. Outgoing S/MIME encrypted emails are able to be scan with anti-virus as additional protection before being send to a recipient. This provides some additional security to help with email security.

Securing email has become a challenge for the basic user end user. Simple steps like installing antivirus, setting security features, and S/MIME have made the basic user's email more secure. This has help to protect against most of the Trojans, viruses and malware. In addition, computer security patches has help to contribute to a more secure email and computer system. End users have found that using these basis steps are a move in the right directions for email security.

Works Cited

Aycock, John. *Spyware and Adware*. Springer Science, 2011.

Erbschloe, Michael. "Trojans, Worms, and Spyware." *A Computer Security Professional's Guide to Malicious Code* (2005): 54-57.

James, Lance. *Phishing Exposed*. Rockland: Syngress, 2005.

Leyden, John. *Sobig-F is fastest growing virus ever*. 21 August 2003. 3 April 2013.

Weitzenkorn, Ben. *Fake Flash Update Installs Feared Banking Trojan*. 31 January 2013. 20 March 2013.

Whitman, Michael E and Herbert J Mattord. *Principles of Information Security Fourth Edition*. Boston: Cengage Learning, 2012.